CLAIMS

1. A parameter generation apparatus for generating an output parameter that is a set of parameters causing no decryption error for an NTRU cryptosystem, the parameter generation apparatus comprising an error-free output parameter generation unit operable to generate the output parameter that does not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error.

2. The parameter generation apparatus according to Claim 1,

wherein the error-free output parameter generation unit includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the error condition information; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters.

3. The parameter generation apparatus according to Claim 2,

wherein the provisional parameter generation unit generates the set of provisional parameters that do not cause any decryption errors, based on an input parameter and the error condition information, said input parameter being a set of parameters for the NTRU cryptosystem that are inputted from outside.

4. The parameter generation apparatus according to Claim 2,

wherein the output parameter generation unit generates the output parameter, using the set of provisional parameters, based on

security determination information and security level information, said security determination information being associated with the lattice constant, and said security level information indicating a level of security against decryption performed by a third party.

5. The parameter generation apparatus according to Claim 4, wherein the output parameter generation unit includes a security determination information holding unit operable to hold the security determination information, and

said security determination information is provided from outside.

6. The parameter generation apparatus according to Claim 4, wherein the output parameter generation unit includes a lattice constant storage unit operable to store one or more lattice constant and security determination information pairs, and

the lattice constant and the security determination information are provided from outside.

7. The parameter generation apparatus according to Claim 6, wherein the output parameter generation unit further includes a security determination information selection unit operable to select one security determination information from said one or more pairs stored in the lattice constant storage unit, based on the lattice constant, and

the output parameter generation unit generates the output parameter, using the selected security determination information and the lattice constant that makes a pair with said selected security determination information.

8. The parameter generation apparatus according to Claim 6, wherein the output parameter generation unit includes:

a modification judgment unit operable to judge whether to modify the set of provisional parameters, based on the lattice constant and the security determination information;

a provisional parameter modification unit operable to generate a modified set of provisional parameters using the set of provisional parameters, when the modification unit judges that the set of provisional parameters should be modified; and

a generation unit operable to generate the output parameter, using the modified set of provisional parameters, based on the security level information.

9. The parameter generation apparatus according to Claim 8,

wherein the provisional parameter modification unit generates the modified set of provisional parameters by modifying a non-negative integer dg, included in the set of provisional parameters, for specifying the number of coefficients in a random polynomial g whose coefficient values equal to 1, said random polynomial g being used for generating a public key polynomial.

10. The parameter generation apparatus according to Claim 2,

wherein the set of provisional parameters and the output parameter are each made up of a set of the following: a degree N in the NTRU cryptosystem; a non-negative integer p; a non-negative integer q; a non-negative integer df for specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1; a non-negative integer dg for specifying the number of coefficients in a random polynomial g whose coefficient values equal to 1, said random polynomial g being used for generating a public key polynomial; and a non-negative integer d for specifying the number of coefficients in a random number polynomial r whose coefficient values equal to 1, said random number polynomial r being used for encrypting a plain text.

11. The parameter generation apparatus according to Claim 10, wherein the provisional parameter generation unit includes an initial security determination information holding unit operable to hold initial security determination information that is associated with time needed to perform decryption, and generates the degree N included in the set of provisional parameters, based on the security level information and said initial security determination information.

12. The parameter generation apparatus according to Claim 10, wherein the provisional parameter generation unit generates the non-negative integer df, the non-negative integer dg, and the non-negative integer d that are included in the set of provisional parameters, based on the security level information and the degree N.

13. The parameter generation apparatus according to Claim 10, wherein the provisional parameter generation unit generates the non-negative integer q included in the set of provisional parameters, based on the error condition information.

14. The parameter generation apparatus according to Claim 10, wherein the output parameter generation unit generates the degree N included in the output parameter, based on the security level information and the security determination information.

15. The parameter generation apparatus according to Claim 1, wherein the error condition information is a conditional expression that indicates the condition for causing no decryption error.

16. The parameter generation apparatus according to Claim 15, wherein the error condition information is the conditional

expression for causing no decryption error that is represented as

$$2 \cdot p \cdot d + 2d \cdot f - 1 < q/2,$$

with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non-negative integer df that is for specifying the number of coefficients in a private key polynomial f whose coefficient values equal to 1, said non-negative integers being for the NTRU cryptosystem.

17. The parameter generation apparatus according to Claim 1, wherein the NTRU cryptosystem is an encryption system for encrypting a plain text and decrypting an encrypted text by a method comprising the following steps:

a selection step of selecting ideals p and q of a ring R that is a group of arrays of dimension N in which addition, subtraction and multiplication are defined;

a generation step of generating elements f and g of the ring R, and generating element F.sub.q which is an inverse of f (mod q), and generating element F.sub.p which is an inverse of f (mod p);

a public key production step of producing a public key that includes h, where h is congruent, mod q, to a product that can be derived using g and F.sub.q;

a private key production step of producing, as a private key, information from which f and F.sub.p can be derived;

an encryption step of producing the encrypted text by encoding the plain text using the public key and element i that is randomly selected from the ring R; and

a decryption step of producing a decrypted text by decrypting the encrypted text using the private key.

18. An encryption system for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption system comprising:

a parameter generation apparatus that includes an error-free output parameter generation unit operable to generate an output parameter that does not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

a public key generation unit operable to generate a public key based on the output parameter generated by the parameter generation apparatus; and

an encryption unit operable to encrypt the plain text based on the public key.

19. A decryption system for generating a decrypted text by decrypting an encrypted text in compliance with an NTRU cryptosystem, the decryption system comprising:

a parameter generation apparatus that includes an error-free output parameter generation unit operable to generate an output parameter that does not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

a private key generation unit operable to generate a private key based on the output parameter generated by the parameter generation apparatus; and

a decryption unit operable to decrypt the encrypted text based on the private key.

20. An encryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key and a decryption key for the NTRU cryptosystem;

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem; and

a decryption apparatus for generating a decrypted text by decrypting the encrypted text,

wherein the parameter generation apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the encryption key and the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key and decryption key,

the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and the encryption key inputted from the key generation apparatus, and

the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation apparatus.

21. An encryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key for the NTRU cryptosystem; and

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem,

wherein the parameter generation apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the encryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key, and

the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and the encryption key inputted from the key generation apparatus.

22. An encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption apparatus comprising:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

an output parameter generation unit operable to generate an output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a parameter transmission unit operable to transmit the output parameter to a decryption apparatus;

an encryption key receiving unit operable to receive, from the decryption apparatus, an encryption key for the NTRU cryptosystem that is generated based on the output parameter; and

an encrypted text generation unit operable to generate the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

23. An encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem, the encryption apparatus comprising:

a parameter receiving unit operable to receive an output parameter that does not cause any decryption errors and that is generated based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error ;

a public key generation unit operable to generate a public key based on the output parameter received by the parameter receiving unit; and

an encryption unit operable to encrypt the plain text based on

the public key.

24. An encryption method for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the encryption method comprising the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating an encryption key for the NTRU cryptosystem based on the output parameter; and

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

25. A program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the program causing a computer to execute the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating an encryption key for the NTRU cryptosystem

based on the output parameter; and

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

26. A decryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating and outputting an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting a decryption key for the NTRU cryptosystem; and

a decryption apparatus for generating a decrypted text by decrypting an encrypted text in compliance with the NTRU cryptosystem,

wherein the parameter generation apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated decryption key, and

the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation

apparatus.

27. A decryption apparatus for generating a decrypted text by decrypting an encrypted text received from an encryption apparatus in compliance with an NTRU cryptosystem, the decryption apparatus comprising:

a parameter receiving unit operable to receive, from the encryption apparatus, an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a generated key generation unit operable to generate an encryption key and a decryption key for the NTRU cryptosystem, using the inputted output parameter, and output the generated encryption key and decryption key;

an encryption key transmission unit operable to transmit the encrypted key to the encryption apparatus; and

a decrypted text generation unit operable to generate the decrypted text by decrypting the encrypted text based on the output parameter and the decryption key.

28. A decryption method for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the decryption method comprising the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating a decryption key for the NTRU cryptosystem based

on the output parameter; and

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key.

29. A program for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the program causing a computer to execute the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating a decryption key for the NTRU cryptosystem based on the output parameter; and

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key.

30. An encryption system using an NTRU cryptosystem, comprising:

a parameter conversion apparatus for converting, into an output parameter, an input parameter that is a set of parameters for the NTRU cryptosystem that are inputted from outside, said output parameter being a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key and a decryption key for the NTRU cryptosystem;

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem;

and

a decryption apparatus for generating a decrypted text by decrypting the encrypted text,

wherein the parameter conversion apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the input parameter and error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the encryption key and the decryption key, using the output parameter inputted from the parameter conversion apparatus, and output the generated encryption key and decryption key,

the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter conversion apparatus and the encryption key inputted from the key generation apparatus, and

the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter conversion apparatus and the decryption key inputted from the key generation apparatus.

31. An encryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating an output parameter from an input parameter that is a set of parameters for the NTRU cryptosystem that are inputted from outside, and outputting the generated output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting an encryption key for the NTRU cryptosystem; and

an encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with the NTRU cryptosystem,

wherein the parameter generation apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the input parameter and error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the encryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated encryption key, and

the encryption apparatus includes an encryption unit operable to generate the encrypted text by encrypting the plain text, using the output parameter inputted from the parameter generation apparatus and the encryption key inputted from the key generation apparatus.

32. An encryption apparatus for generating an encrypted text by encrypting a plain text in compliance with an NTRU cryptosystem,

the encryption apparatus comprising:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, said input parameter and error condition information being provided in advance;

an output parameter generation unit operable to generate an output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a parameter transmission unit operable to transmit the output parameter to a decryption apparatus;

an encryption key receiving unit operable to receive, from the decryption apparatus, an encryption key for the NTRU cryptosystem that is generated based on the output parameter; and

an encrypted text generation unit operable to generate the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

33. An encryption method for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the encryption method comprising the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, said input parameter and error condition information being provided in advance;

generating an output parameter that is a set of parameters

causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating an encryption key for the NTRU cryptosystem based on the output parameter; and

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

34. A program for generating an encrypted text by encrypting a plain text in compliance with NTRU cryptosystem, the program causing a computer to execute the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, said input parameter and error condition information being provided in advance;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating an encryption key for the NTRU cryptosystem based on the output parameter; and

generating the encrypted text by encrypting the plain text, based on the output parameter and the encryption key.

35. A decryption system using an NTRU cryptosystem, comprising:

a parameter generation apparatus for generating an output parameter from an input parameter that is a set of parameters for

the NTRU cryptosystem that are inputted from outside, and outputting the generated output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem;

a key generation apparatus for generating and outputting a decryption key for the NTRU cryptosystem; and

a decryption apparatus for generating a decrypted text by decrypting an encrypted text in compliance with the NTRU cryptosystem,

wherein the parameter generation apparatus includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on the input parameter and error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and

an output parameter generation unit operable to generate the output parameter, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and output the generated output parameter,

the key generation apparatus includes a generated key output unit operable to generate the decryption key, using the output parameter inputted from the parameter generation apparatus, and output the generated decryption key, and

the decryption apparatus includes a decryption unit operable to generate the decrypted text by decrypting the encrypted text, using the output parameter inputted from the parameter generation apparatus and the decryption key inputted from the key generation apparatus.

36. A decryption method for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the decryption method comprising the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, said input parameter and error condition information being provided in advance;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating a decryption key for the NTRU cryptosystem based on the output parameter; and

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key.

37. A program for generating a decrypted text by decrypting an encrypted text in compliance with NTRU cryptosystem, the program causing a computer to execute the following steps of:

generating a set of provisional parameters that do not cause any decryption errors, based on an input parameter that is a set of parameters for the NTRU cryptosystem and error condition information indicating a condition for causing no decryption error, said input parameter and error condition information being provided in advance;

generating an output parameter that is a set of parameters causing no decryption error for the NTRU cryptosystem, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters, and outputting said generated output parameter;

generating a decryption key for the NTRU cryptosystem based on the output parameter; and

generating the decrypted text by decrypting the encrypted text, based on the output parameter and the decryption key.